



(19) RU (11) 2 166 792 (13) С1
(51) МПК⁷ G 06 F 12/14, 15/16, 11/00

РОССИЙСКОЕ АГЕНТСТВО
ПО ПАТЕНТАМ И ТОВАРНЫМ ЗНАКАМ

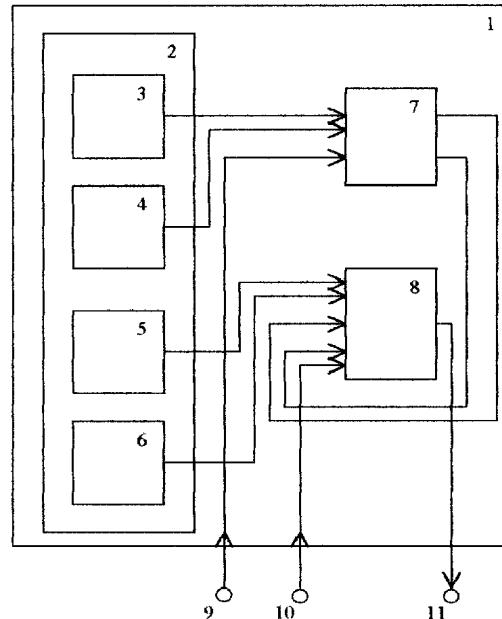
(12) ОПИСАНИЕ ИЗОБРЕТЕНИЯ К ПАТЕНТУ РОССИЙСКОЙ
ФЕДЕРАЦИИ

(21), (22) Заявка: 99122295/09, 25.10.1999
(24) Дата начала действия патента: 25.10.1999
(43) Дата публикации заявки: 10.05.2001
(46) Дата публикации: 10.05.2001
(56) Ссылки: US 5892900 A, 06.04.1999. RU
2067313C1, 27.09.1996. US 5809543 A,
15.09.1998. US 5815722 A, 29.09.1998. US
5832511 A, 11.03.1998.
(98) Адрес для переписки:
197101, Санкт-Петербург, Большой пр-т П.С.,
д.53, кв.14, Щеглову А.Ю.

(71) Заявитель:
Щеглов Андрей Юрьевич
(72) Изобретатель: Щеглов А.Ю.
(73) Патентообладатель:
Щеглов Андрей Юрьевич

(54) СИСТЕМА ЗАЩИТЫ РАБОЧИХ СТАНЦИЙ, ИНФОРМАЦИОННЫХ И ФУНКЦИОНАЛЬНЫХ СЕРВЕРОВ
ВЫЧИСЛИТЕЛЬНЫХ СИСТЕМ И СЕТЕЙ С ДИНАМИЧЕСКИМИ СПИСКАМИ САНКЦИОНИРОВАННЫХ
СОБЫТИЙ

(57) Реферат:
Изобретение относится к вычислительной
технике, а именно к информационным
вычислительным системам и сетям, и может
быть использовано для защиты
информационных ресурсов в рабочих
станциях, информационных и
функциональных серверах. Техническим
результатом является повышение уровня
защищенности рабочих станций,
функциональных и информационных
серверов, обеспечиваемого устанавливаемой
на них системой защиты, реализующей
принципы контроля целостности информации,
асинхронного контроля целостности программ
и данных. Для этого система защиты
информации содержит блок памяти, блок
формирования текущих контрольных сумм,
блок сравнения контрольных сумм, M блоков
формирования списков текущих событий, M
блоков сравнения списков текущих и
санкционированных событий, M блоков
выработки команды на "уничтожение"
(прекращение) текущего события, блок
выработки сигнала сравнения контрольных
сумм, M блоков разграничения и контроля
прав запуска события, M блоков корректировки
списка санкционированных событий. 3 ил.



Фиг. 1

R
U
2
1
6
6
7
9
2
C
1

R
U
~
1
6
6
7
9
2
C
1



(19) RU (11) 2 166 792 (13) C1
(51) Int. Cl.⁷ G 06 F 12/14, 15/16, 11/00

RUSSIAN AGENCY
FOR PATENTS AND TRADEMARKS

(12) ABSTRACT OF INVENTION

(21), (22) Application: 99122295/09, 25.10.1999

(24) Effective date for property rights: 25.10.1999

(43) Application published: 10.05.2001

(46) Date of publication: 10.05.2001

(98) Mail address:
197101, Sankt-Peterburg, Bol'shoj pr-t P.S.,
d.53, kv.14, Shcheglov A.Ju.

(71) Applicant:
Shcheglov Andrej Jur'evich

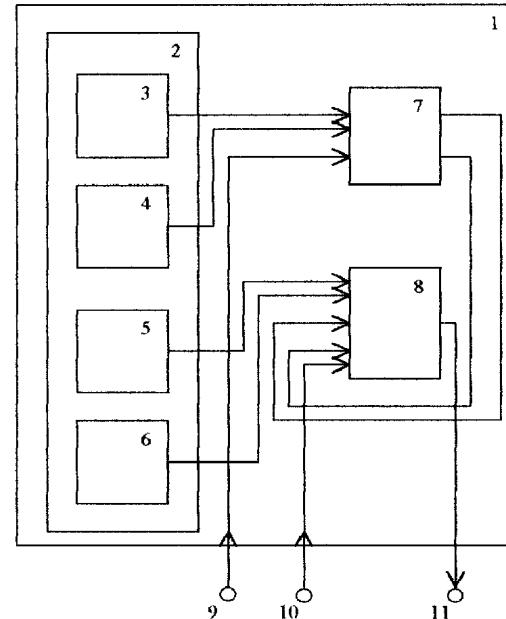
(72) Inventor: Shcheglov A.Ju.

(73) Proprietor:
Shcheglov Andrej Jur'evich

(54) PROTECTIVE SYSTEMS OF WORKSTATIONS, INFORMATION AND FUNCTIONAL SERVERS OF COMPUTER SYSTEMS AND NETWORKS WITH DYNAMIC LISTS OF AUTHORIZED EVENTS

(57) Abstract:

FIELD: computer engineering; data computing systems and networks. SUBSTANCE: system has memory unit, current check sum shaping unit, check sum comparison unit, M units for shaping lists of current-events, M units for shaping lists of current and authorized events, M units generating command for deleting (stopping) current event, check-sum comparison signal generating unit, M units for delimiting and checking event starting rights, M units for correcting authorized events list. System implements principles of data integrity check-up, asynchronous control of program and data integrity. EFFECT: improved protection level. 3 dwg



Фиг.1

RU 2166792 C1

RU 2166792 C1

Изобретение относится к вычислительной технике, а именно к информационным вычислительным системам и сетям, и может быть использовано для защиты информационных ресурсов в рабочих станциях, информационных и функциональных (например, выделенный сервер безопасности, Proxy-сервер, межсетевой экран и т.д.) серверах.

Известна система защиты информационных ресурсов вычислительной системы и сети Secret Net (см. "Система разграничения доступа Secret Net. Руководство пользователя, 1996"). Она представляет собою программный комплекс, устанавливаемый на автономный компьютер, либо на компьютеры, объединенные в вычислительную сеть. Система решает задачу контроля целостности (неискаженности) программ и данных при включении системы.

Наиболее близкой по технической сущности к заявляемой (прототипом) является система защиты информационных ресурсов SvinKa-i (разработка ЗАО "Relcom-alpha" (Москва)), описана на сайте фирмы, расположенному по адресу <http://WWW.alpha.ru/Products/SvinKa-i>.

Система представлена на фиг. 1. Система защиты информации 1 включает блок памяти 2, содержащий блок функционального программного обеспечения (ФПО) 3, блок данных 4, блок хранения контрольных сумм ФПО 5, блок хранения контрольных сумм данных 6, кроме того, блок формирования текущих контрольных сумм 7, блок сравнения контрольных сумм 8, причем выход блока ФПО 3 (первый выход блока памяти 2) соединен с первым входом блока формирования текущих контрольных сумм 7, выход блока данных 4 (второй выход блока памяти 2) - со вторым входом блока формирования текущих контрольных сумм 7, третий вход которого соединен с управляющим входом сравнения контрольных сумм 9 (первым входом системы защиты информации 1), выход блока хранения контрольных сумм ФПО 5 (третий выход блока памяти 2) соединен с первым входом блока сравнения контрольных сумм 8, выход блока хранения контрольных сумм данных 6 (четвертый выход блока памяти 2) - со вторым входом блока сравнения контрольных сумм 8, третий вход которого соединен с первым, а четвертый вход - со вторым выходами блока формирования текущих контрольных сумм 7, пятый вход блока сравнения контрольных сумм 8 соединен с управляющим входом сравнения контрольных сумм 10 (вторым входом системы защиты информации 1), выход блока сравнения контрольных сумм 8 соединен с управляющим выходом результата сравнения контрольных сумм 11 (выходом системы защиты 1).

Защита информации осуществляется в части контроля целостности (неискаженности) программ (ФПО) и данных, что реализуется следующим образом. В блоках памяти 5 и 6 соответственно хранятся контрольные суммы контролируемых блоков 3 и 4. По команде с управляющего входа 9 блоком 7 формируются текущие контрольные суммы информации, хранящейся в блоках 3 и 4, и по команде с управляющего входа 10 полученные блоком 7 текущие контрольные суммы сравниваются с соответствующими контрольными суммами, находящимися в блоках 5 и 6. Блоком 8

сравниваются текущие и исходные контрольные суммы, результат сравнения выдается на управляющий выход 11. При обнаружении факта несовпадения контрольных сумм фиксируется факт несанкционированного доступа (НСД) к информации.

Недостатком системы является неэффективное использование механизма контроля целостности, что обуславливается следующим - факт НСД фиксируется лишь при искажении злоумышленником информации (при прочтении информации без искажения факт НСД не регистрируется), использование данного механизма не позволяет предотвращать НСД. Кроме того, не эффективно использование механизма контроля целостности программ и данных в принципе, т.к. контроль не искаженности файловой системы требует больших затрат времени, что не позволяет проводить его в системе часто, редкое же проведение контроля не позволяет эффективно противодействовать угрозам. Кроме того, рассматриваемая система не позволяет противодействовать таким видам угроз как закладки и ошибки, в том числе, в программном обеспечении.

Целью изобретения является повышение уровня защищенности рабочих станций, функциональных и информационных серверов, обеспечиваемого устанавливаемой на них системой защиты, реализующей принципы контроля целостности информации, за счет максимально эффективной реализации возможности не только обнаруживать, но и предотвращать НСД к информации, обеспечиваемой реализацией метода контроля динамических списков санкционированных событий, при этом появляется возможность обнаруживать факт НСД и при отсутствии искажения информации злоумышленником, причем, в том числе, реализуется и возможность обнаружения и предотвращения факта НСД и при использовании злоумышленником ошибок и закладок, а так же с целью повышения эффективности контроля целостности программ и данных, за счет использования вторичных признаков, обеспечивающих возможность асинхронного контроля целостности программ и данных.

Достигается это тем, что в систему защиты информации, содержащую блок памяти, содержащий блок функционального программного обеспечения (ФПО), блок данных, блок хранения контрольных сумм ФПО, блок хранения контрольных сумм данных, и кроме блока памяти - блок формирования текущих контрольных сумм, блок сравнения контрольных сумм, причем выход блока ФПО - первый выход блока памяти соединен с первым входом блока формирования текущих контрольных сумм, выход блока данных - второй выход блока памяти - со вторым входом блока формирования текущих контрольных сумм, третий вход которого соединен с управляющим входом сравнения контрольных сумм - первым входом системы защиты информации, выход блока хранения контрольных сумм ФПО - третий выход блока памяти соединен с первым входом блока сравнения контрольных сумм, выход блока хранения контрольных сумм данных -

четвертый выход блока памяти - со вторым входом блока сравнения контрольных сумм, третий вход которого соединен с первым, а четвертый вход - со вторым выходами блока формирования текущих контрольных сумм, выход блока сравнения контрольных сумм соединен с управляющим выходом результата сравнения контрольных сумм - выходом системы защиты, дополнительно введены: в блок памяти - M блоков хранения списков санкционированных событий, M блоков хранения контрольных сумм списков санкционированных событий, кроме того в систему защиты введены - M блоков формирования списков текущих событий, M блоков сравнения списков текущих и санкционированных событий, M блоков выработки команды на "уничтожение" (прекращение) текущего события, блок выработки сигнала сравнения контрольных сумм, M блоков разграничения и контроля прав запуска события, M блоков корректировки списка санкционированных событий, причем выходы блоков хранения списков санкционированных событий - выходы с 5 по M+4 блока памяти соединены с входами с 4 по M+3 блока формирования текущих контрольных сумм с M первыми входами блоков сравнения списков текущих и санкционированных событий и блоков выработки команды на "уничтожение" (прекращение) текущего события, первые выходы блоков формирования списков текущих событий соединены с M информационными входами регистрации текущих событий - M третьими входами системы защиты информации, вторые выходы соединены с M управляющими входами регистрации текущих событий - M четвертыми входами системы защиты, выходы соответственно соединены со вторыми входами блоков сравнения списков текущих и санкционированных событий, третьи выходы которых соединены с M управляющими входами сравнения текущих и санкционированных событий - M пятными выходами системы защиты, выходы соединены с M управляющими выходами результатов сравнения списков текущих и санкционированных событий - M вторыми выходами системы защиты информации, со вторыми входами блоков выработки команды на "уничтожение" (прекращение) текущего события, с первыми M входами блока выработки сигнала сравнения контрольных сумм, M+1 вход которого соединен с управляющим входом сравнения контрольных сумм - вторым входом системы защиты информации, выход соединен с пятым входом блока сравнения контрольных сумм, выходы блоков выработки команды на "уничтожение" (прекращение) текущего события соединены с M управляющими выходами "уничтожения" (прекращения) текущего события, выходы блоков хранения контрольных сумм списков санкционированных событий соединены со входами с 6 по M+5 блока сравнения контрольных сумм, входы M блоков разграничения и контроля прав запуска события соединены с соответствующими M входами запроса и согласования прав запуска события, выходы - с первыми входами M блоков корректировки списков санкционированных событий, вторые M входов - с M входами уведомления о завершении события, первые M выходов - соответственно

со входами M блоков хранения списков санкционированных событий, вторые M выходов - с M выходами разрешения запуска события, третьи M выходов - соответственно с четвертыми выходами M блоков сравнения списков текущих и санкционированных событий.

Схема системы защиты информации 1 приведена на фиг. 2, она содержит: блок памяти 2, содержащий блок функционального программного обеспечения (ФПО) 3, блок данных 4, блок хранения контрольных сумм ФПО 5, блок хранения контрольных сумм данных 6, M блоков хранения списков санкционированных событий 12, M блоков хранения контрольных сумм списков санкционированных событий 13, кроме того, система защиты информации 1 содержит: блок формирования текущих контрольных сумм 7, блок сравнения контрольных сумм 8, M блоков формирования списков текущих событий 14, M блоков сравнения списков текущих и санкционированных событий 15, M блоков выработки команды на "уничтожение" (прекращение) текущего события 16, блок выработки сигнала сравнения контрольных сумм 17, M блоков разграничения и контроля прав запуска события 18, M блоков корректировки списка санкционированных событий 19, причем выход блока ФПО 3 - первый выход блока памяти 2 соединен с первым входом блока формирования текущих контрольных сумм 7, выход блока данных 4 -второй выход блока памяти 2 - со вторым входом блока формирования текущих контрольных сумм 7, третий вход которого соединен с управляющим входом сравнения контрольных сумм 9 - первым входом системы защиты информации 1, выход блока хранения контрольных сумм ФПО 5 - третий выход блока памяти 2 соединен с первым входом блока сравнения контрольных сумм 8, выход блока хранения контрольных сумм данных 6 - четвертый выход блока памяти 2 - со вторым входом блока сравнения контрольных сумм 8, третий вход которого соединен с первым, а четвертый вход - со вторым выходами блока формирования текущих контрольных сумм 7, выход блока сравнения контрольных сумм 8 соединен с управляющим выходом результата сравнения контрольных сумм 11 - выходом системы защиты 1, выходы блоков хранения списков санкционированных событий 12 - выходы с 5 по M+4 блока памяти 2 соединены с входами с 4 по M+3 блока формирования текущих контрольных сумм 7, с M первыми входами блоков сравнения списков текущих и санкционированных событий 15 и блоков выработки команды на "уничтожение" (прекращение) текущего события 16, первые выходы блоков формирования списков текущих событий 14 соединены с M информационными входами регистрации текущих событий 20 - M третьими входами системы защиты информации 1, вторые выходы соединены с M управляющими входами регистрации текущих событий 21- M четвертыми входами системы защиты 1, выходы соответственно соединены со вторыми входами блоков сравнения списков текущих и санкционированных событий 15, третьи выходы которых соединены с M управляющими входами сравнения текущих и санкционированных событий 22 - M пятными выходами системы защиты 1, выходы соединены с M управляющими выходами

результатов сравнения списков текущих и санкционированных событий 25 - М вторыми выходами системы защиты информации 1, со вторыми входами блоков выработки команды на "уничтожение" (прекращение) текущего события 16, с первыми М входами блока выработки сигнала сравнения контрольных сумм 17, М+1 вход которого соединен с управляющим входом сравнения контрольных сумм 10 - вторым входом системы защиты информации 1, выход соединен с пятым входом блока сравнения контрольных сумм 8, выходы блоков выработки команды на "уничтожение" (прекращение) текущего события 16 соединены с М управляющими выходами "уничтожения" (прекращения) текущего события 26, выходы блоков хранения контрольных сумм списков санкционированных событий 13 соединены со входами с 6 по М+5 блока сравнения контрольных сумм 8, выходы М блоков разграничения и контроля прав запуска события 18 соединены с соответствующими М входами запроса и согласования прав запуска события 23, выходы - с первыми входами М блоков корректировки списков санкционированных событий 19, вторые М входов - соответственно со входами М блоков хранения списков санкционированных событий 12, вторые М выходов - с М выходами разрешения запуска события 27, третьи М выходов - соответственно с четвертыми входами М блоков сравнения списков текущих и санкционированных событий 15.

Работает система следующим образом. Задача защиты информации в рамках предлагаемого метода, реализуемого заявляемым устройством, сводится к контролю не искаженности или целостности списков санкционированных событий, программ и данных (т.е. в основе предлагаемого подхода положен многофункциональный последовательный контроль целостности). Особенностью подхода является формирование и отслеживание списков санкционированных событий в процессе функционирования системы. Здесь списки заданы не статически, а они динамические - события разрешаются к запуску и "уничтожаются" при непрерывном контроле их разрешенности в системе. Например, рассмотрим в качестве санкционированного события - процесс некой сетевой службы, пусть FTP. Изначально, данный процесс запрещен к запуску - отсутствует в исходном списке санкционированных событий. Лишь после идентификации и аутентификации пользователя и его намерений (реализуется механизм разграничения и контроля прав доступа, в том числе, и основанный на мандатном принципе управления) процесс вносится в список санкционированных событий - разрешается к запуску в системе - на одну сессию FTP. Корректируется список санкционированных событий, который непрерывно контролируется в системе. Контроль списков санкционированных событий может осуществляться синхронно (по расписанию), либо асинхронно, реализуемый по принципу "при условии, что...", но не в момент их формирования (изменения). В общем случае, идея подхода отображена на

фиг. 3 и состоит в том, что при доступе к информации осуществляется последовательный быстрый анализ не искаженности (контролируется целостность) списков событий, причем в данном случае - динамических. К достоинствам использования динамических списков санкционированных событий может быть отнесено повышение уровня защищенности системы, обусловливаемое тем, что в каждый момент времени ее функционирования, в системе разрешаются к запуску лишь действительно необходимые события (например, процессы), а не разрешенные для всех случаев функционирования системы, что может быть реализовано при статических списках. При несанкционированном доступе, по крайней мере, одно событие из анализируемого набора списков должно нарушаться (в противном случае имеем санкционированный доступ к информации) - быть несанкционированным. К подобным спискам могут быть отнесены:

- 20 список санкционированных пользователей;
- таблицы прав доступа пользователей (к файлам, каталогам, устройствам, серверам и т.д.), мандатов;
- список разрешенных к запуску процессов;
- 25 список открытых портов;
- список подключенных устройств;
- список разрешенных для взаимодействие IP-адресов, либо DNS-имен,
- состояние ключей реестра и т.д.

Идея подхода состоит в том, что (это подтвердили исследования) фоновый анализ списков санкционированных событий осуществляется столь быстро, что позволяет предотвратить несанкционированное воздействие (например, несанкционированного пользователя, незарегистрированный процесс и т.д.) до момента доступа злоумышленника к информации, чем предотвращается попытка НСД.

Отличие в использовании предложенной технологии для альтернативных 40 операционных сред (операционных систем) состоит лишь в наборе списков (уровней контроля целостности) несанкционированных событий, которые могут поддерживаться конкретными операционными системами.

Отличие в использовании предложенной 45 технологии для альтернативных вариантов реализации политики информационной безопасности предприятия состоит лишь в наборе контролируемых списков (уровней контроля целостности), в очередности и периодичности их контроля.

Сказанное позволяет утверждать о 50 возможности унификации предложенного подхода для альтернативных применений, где условия использования системы могут учитываться средствами настройки ее параметров, в рамках единого унифицированного подхода, проиллюстрированного на фиг. 3.

Теперь рассмотрим, как описанный метод 55 реализуется схемой, приведенной на фиг. 2. Схема предполагает введение в систему защиты в общем случае М списков санкционированных событий. Блоки 12 хранят в памяти собственно списки санкционированных событий. По команде с управляющего входа 21 в заданной последовательности и в заданные моменты времени (это определяется очередностью и

периодичностью подачи сигналов на M входов 21) блоками 14 с информационных входов 20 формируются (регистрируются) текущие списки санкционированных событий (например,читываются таблицы зарегистрированных пользователей и таблицы разграничения прав доступа, таблицы подключенных устройств, фиксируются запущенные процессы, программно открытые порты и т.д.), которые по команде со входа системы 22 блоками 15 сравниваются со списками санкционированных событий, расположенных в блоках 12. Блоки 15 вырабатывают управляющие сигналы на выход 25, по которым затем обеспечивается реакция, например прописанная в соответствующем командном файле - файле /bat/ операционной системы. Кроме того, данные сигналы поступают в блоки 16 и блок 17. Блоки 16 формируют сигналы на выходе 26, предназначенные для "уничтожения" несанкционированных действий, например сигнал завершения запущенного несанкционированного процесса, сигнал восстановления исходной таблицы разрешенных пользователей, прав доступа пользователей, сигнал на программное закрытие соответствующего порта и т.д. Блок 17 вырабатывает сигнал сравнения текущих и исходных контрольных сумм ФПО, данных и собственно контрольных сумм списков санкционированных событий (которые также могут быть изменены), хранящихся в блоках 13. Таким образом, в рассматриваемой системе допускается два режима контроля целостности программ и данных - синхронно - при включении системы, по расписанию - с входа 10, и асинхронно - здесь сигналом проверки совпадения контрольных сумм является условие искажения (нарушения целостности) списка санкционированных событий - с выхода блока 15. Данная особенность функционирования системы весьма важна, т.к. контроль больших объемов данных может занимать много времени (минуты), в то время, как контроль списка санкционированных событий занимает миллисекунды. Использование данного подхода позволяет существенно повышать производительность системы при асинхронной процедуре запуска контроля целостности программ и данных. В формировании списков в блоках 12 используются M блоков 18 и M блоков 19 (соответственно, в общем случае, на каждый список свои блоки 12, 18, 19). При запросе запуска события, например процесса, пользователем на вход 23 подаются его регистрационные параметры, например, идентификатор, пароль, запрашиваемый сервис (процесс, имя файла и т.д.), мандат (при реализации мандатного управления доступом). При разрешении запуска запрашиваемого процесса (блок 18 решает задачу разграничения прав доступа) через блок 19 корректируется содержимое соответствующего блока 12 и после окончания корректировки с выхода 27 разрешает запустить событие (либо не разрешает, выдавая пользователю отрицательный ответ). При этом на все время корректировки списка санкционированных событий с выхода блоков 19 запрещается сравнение на блоках 15 для соответствующего события текущего и санкционированного списков событий. По завершении события со входа 24 процедура

корректировки вписка проводится вновь, аналогично, но уже в части исключения завершенного события из исходного списка (из соответствующего блока 12). После завершения корректировки списков, сравнение текущих и уже откорректированных списков событий продолжается, контролируя правильность функционирования системы.

Актуальность современной проблемы борьбы с ошибками и закладками обусловливается тем, что с, одной стороны, их практически невозможно выявить, с другой стороны, в частности для ошибок, ввиду высокой интенсивности смены программных средств на рынке информационных технологий, как следствие, сокращения сроков разработки, характерно повышение их доли в современных программных средствах. Вероятность наличия закладок в программных средствах, наверное, величина относительно постоянная, больше зависит от области практического использования системы. Для поиска ошибок сегодня перед введением системы в эксплуатацию используют соответствующие программы-тестеры, содержащие некоторую базу данных известных для средств, подобных анализируемому, ошибок за несколько лет. Недостаток данного подхода связан с невозможностью поиска новых ошибок, а лишь анализ наличия известных. Поэтому, с точки зрения поиска ошибок, можем сказать, что, к сожалению, большинство из них выявляется именно в процессе функционирования систем, кстати говоря, это в полной мере иллюстрируют все время появляющиеся "заплатки" на широко используемых сегодня операционных системах и других программных средствах. Другими словами, говорить о высоком уровне защищенности от угроз, связанных с ошибками в современных программных средствах, наверное, не представляется возможным. Безопасными с точки зрения рассматриваемых угроз программы становятся лишь после некоторого (порядка, достаточно продолжительного) времени их эксплуатации и их "тестирования" злоумышленниками. И лишь когда же злоумышленники, наконец "выдохнутся", что можно оценить по соответствующей статистике атак и взломов, можно говорить об относительной безопасности программного средства с точки зрения рассматриваемых угроз. К сожалению, к этому моменту данное средство уже устаревает и требует замены на новое, еще более сложное и, как правило, разработанное в более сжатые сроки, и, как следствие, содержащее еще большее количество ошибок. Наверное, не более утешительна ситуация и с поиском закладок, несмотря на то, что их число в программном средстве ограничено. Эти угрозы, в отличие от ошибок, практически невозможно отыскать на этапе тестирования технического средства, предшествующем его внедрению. Это обусловлено тем, что закладки, как правило, устанавливают квалифицированные программисты, предпринимая при этом все необходимые меры для усложнения их поиска. К сожалению, несмотря на непрекращающиеся исследования в области поиска закладок, на сегодняшний день можно утверждать, что эффективные подходы к поиску закладок отсутствуют, авторам исследования даже не известен

сколько-нибудь обоснованный математический аппарат, позволяющий формализовать данный процесс и количественно оценить результат исследований.

Таким образом, важнейшим вопросом является реализуемый в системе метод защиты информации - метод, позволяющий эффективно бороться с ошибками и закладками в программном обеспечении. В общем случае возможны два варианта:

Первый - обнаружение факта несанкционированного доступа к информации (изменение данных, файлов, программ и т.п.). В этом случае основная нагрузка ложится на систему обеспечения целостности. Недостаток данного подхода состоит в том, что может фиксироваться лишь факт изменения информации, заметим, что неважно, каким образом произведенный - за счет использования ошибки, либо закладки.

Второй - предотвращение (не допущение) несанкционированного доступа путем анализа косвенных признаков (появление подозрительных процессов, попыток изменения памяти, регистрации новых пользователей и т.д.). Здесь большая роль отводится аудиту событий. Идея использования данного метода состоит в следующем. Использует ли злоумышленник ошибку, либо закладку в программном обеспечении, он должен совершить некоторые неправомерные действия (в противном случае, он санкционированный пользователь, функционирующий в рамках разрешенных ему прав), например, завести нового пользователя, присвоить себе как пользователю более высокие права доступа, запустить несанкционированный процесс, открыть порт, изменить некоторые параметры реестра и т.д. Метод состоит в том, чтобы в фоновом режиме контролировать списки санкционированных событий, восстанавливая их в случае обнаружения искажений с соответствующими функциональными реакциями (например, завершить процесс, закрыть порт, восстановить состояние реестра, базы данных прав доступа пользователей и т. д.). При высокой эффективности подобного контроля (заметим, что данные списки, как правило, невелики) появляется возможность предотвращать действия злоумышленника, вне зависимости от природы его несанкционированного доступа к информации, в том числе и с использованием ошибок и закладок.

Блоки, используемые в заявляемой системе защиты, могут быть реализованы следующим образом.

Блоки 3, 4, 5, 6, 12, 13 представляют собою области, либо отдельные блоки памяти: либо оперативный, либо расположенной на внешних носителях - представляют собою запомненные массивы данных.

Блок 7 - это программное, либо аппаратное средство подсчета контрольной суммы. Данный блок хранит текущее значение контрольной суммы до поступления очередной команды на подсчет текущей контрольной суммы.

Блок 8 - это программное, либо аппаратное средство попарного сравнения значений контрольных сумм.

Блок 14 - это программные, либо аппаратные блоки считывания, либо анализа

списков текущих событий, например, программа считывания таблиц из требуемых областей памяти, стандартные программы выявления открытых портов, запущенных процессов и т.д.

Блок 15 - это программное, либо аппаратное средство построчного сравнения двух таблиц (санкционированных и текущих событий) с фиксированием несовпадений.

Блоки 16 - это программные, либо аппаратные блоки выработки команды на "уничтожение" несанкционированного события - здесь, в зависимости от контролируемых событий, возможны различные реализации, например, восстановление исходной строки таблицы в таблицах разрешенных пользователей, прав доступа, подключенных устройств и т.д., либо запуска обработки стандартной программы завершения несанкционированного процесса, программного закрытия порта и т.д.

Блок 17 - это программное, либо аппаратное средство выработки сигнала на сравнение контрольных сумм - реализуется некоторое правило "Математической логики", в простейшем случае - правило "ИЛИ", тогда обнаружение искажения любого списка приводит к сравнению контрольных сумм.

Блок 18 - это программное либо аппаратное средство, решающее задачу разграничения прав доступа с выработкой соответствующих управляющих сигналов (подобный блок реализуется в любой системе разграничения прав доступа, в частности, в аналоге) - система Secret Net.

Блок 19 - это программное, либо аппаратное средство управления записью информации в память.

Таким образом, реализация всех используемых блоков достигается стандартными средствами, базирующимися на классических принципах реализации основ вычислительной техники.

К достоинствам предлагаемой системы защиты информации может быть отнесено следующее.

1. Реализация принципиально нового подхода к защите информации, в основе которого лежит реализация принципа контроля целостности.

2. Существенное повышение эффективности защиты при использовании предложенного подхода, за счет реализации динамических списков санкционированных событий, что приводит к их минимизации (оптимальному заданию) в каждый момент времени функционирования системы.

3. Появление принципиально новой возможности защиты информации не только от попыток злоумышленника обойти встроенные средства защиты информации, но и от попыток использовать ошибки и закладки в программном обеспечении и аппаратных средствах. По существу, для заявляемой системы защиты не является важным то, каким образом злоумышленник пытается преодолеть защиту.

4. Принципиально новая возможность эффективного контроля целостности программ и данных, обусловливаемая возможностью асинхронного запуска данной медленной процедуры контроля, при условии обнаружения попыток НСД по косвенным признакам - попыткам искажения списков санкционированных событий, контроль

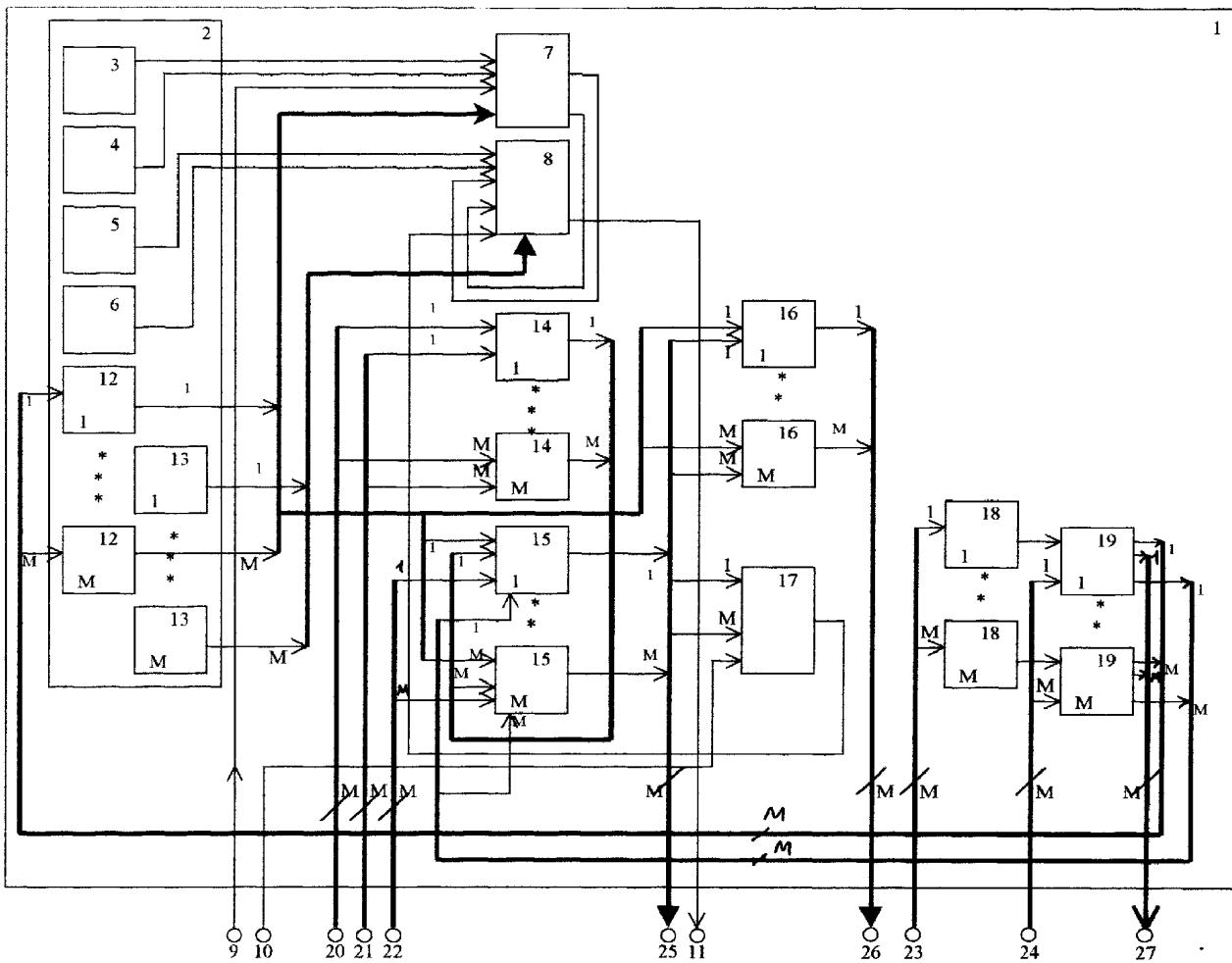
целостности которых осуществляется в тысячи раз быстрее, чем контроль программ и данных. Данное достоинство следует рассматривать не как возможность повышения эффективности процедуры контроля целостности, а как возможность ее использования в принципе, т.к. в противном случае, при использовании подобной процедуры, информационная система начинает работать на собственную защиту.

Формула изобретения:

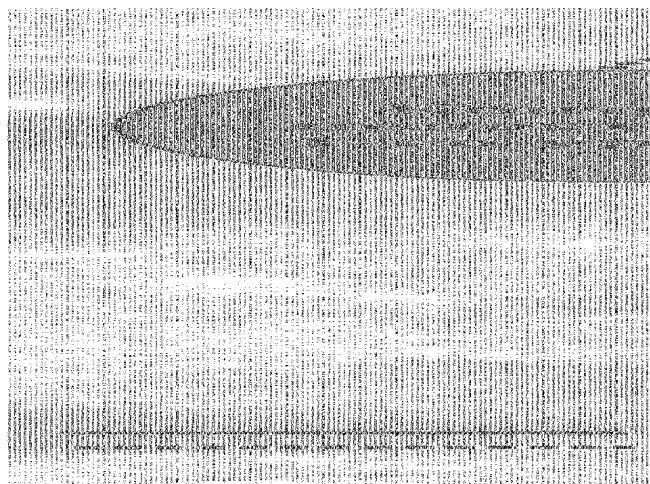
Система защиты информации, содержащая блок памяти, содержащий блок функционального программного обеспечения (ФПО), блок данных, блок хранения контрольных сумм ФПО, блок хранения контрольных сумм данных, и кроме блока памяти - блок формирования текущих контрольных сумм, блок сравнения контрольных сумм, причем выход блока ФПО - первый выход блока памяти соединен с первым входом блока формирования текущих контрольных сумм, выход блока данных - второй выход блока памяти - со вторым входом блока формирования текущих контрольных сумм, третий вход которого соединен с управляющим входом сравнения контрольных сумм - первым входом системы защиты информации, выход блока хранения контрольных сумм ФПО - третий выход блока памяти соединен с первым входом блока сравнения контрольных сумм, выход блока хранения контрольных сумм данных - четвертый выход блока памяти - со вторым входом блока сравнения контрольных сумм, третий вход которого соединен с первым, а четвертый вход - со вторым выходами блока формирования текущих контрольных сумм, выход блока сравнения контрольных сумм соединен с управляющим выходом результата сравнения контрольных сумм - выходом системы защиты, дополнительно введены: в блок памяти - M блоков хранения списков санкционированных событий, M блоков хранения контрольных сумм списков санкционированных событий, кроме того, в систему защиты введены M блоков формирования списков текущих событий, M блоков сравнения списков текущих и санкционированных событий, M блоков выработки команды на "уничтожение" (прекращение) текущего события, блок выработки сигнала сравнения контрольных сумм, M блоков разграничения и контроля прав запуска события, M блоков корректировки списка санкционированных событий, причем выходы блоков хранения списков

санкционированных событий - выходы с 5 по M + 4 блока памяти соединены с входами с 4 по M + 3 блока формирования текущих контрольных сумм, с M первыми входами блоков сравнения списков текущих и санкционированных событий и блоков выработки команды на "уничтожение" (прекращение) текущего события, первые выходы блоков формирования списков текущих событий соединены с M информационными входами регистрации текущих событий - M третьими входами системы защиты информации, вторые выходы соединены с M управляющими входами регистрации текущих событий - M четвертыми входами системы защиты, выходы соответственно соединены со вторыми выходами блоков сравнения списков текущих и санкционированных событий, третьи выходы которых соединены с M управляющими входами сравнения текущих и санкционированных событий - M пятыми входами системы защиты, выходы соединены с M управляющими выходами результатов сравнения списков текущих и санкционированных событий - M вторыми выходами системы защиты информации, со вторыми выходами блоков выработки команды на "уничтожение" (прекращение) текущего события, с первыми M входами блока выработки сигнала сравнения контрольных сумм, M + 1 вход которого соединен с управляющим входом сравнения контрольных сумм - вторым входом системы защиты информации, выход соединен с пятым входом блока сравнения контрольных сумм, выходы блоков выработки команды на "уничтожение" (прекращение) текущего события соединены с M управляющими выходами "уничтожения" (прекращения) текущего события, выходы блоков хранения контрольных сумм списков санкционированных событий соединены со входами с 6 по M + 5 блока сравнения контрольных сумм, входы M блоков разграничения и контроля прав запуска события соединены с соответствующими M входами запроса и согласования прав запуска события, выходы - с первыми входами M блоков корректировки списков санкционированных событий, вторые M входов - с M входами уведомления о завершении события, первые M выходов - соответственно со входами M блоков хранения списков санкционированных событий, вторые M выходов - с M выходами разрешения запуска события, третьи M выходов - соответственно с четвертыми входами M блоков сравнения списков текущих и санкционированных событий.

R U 2 1 6 6 7 9 2 C 1



Фиг.2



R U 2 1 6 6 7 9 2 C 1